PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07C 9/00 — A1

(11) International Publication Number: **WO 99/39310**

(43) International Publication Date: 5 August 1999 (05.08.99)

(21) International Application Number: PCT/US99/01727

(22) International Filing Date: 28 January 1999 (28.01.99)

(30) Priority Data:
60/073,166 30 January 1998 (30.01.98) US

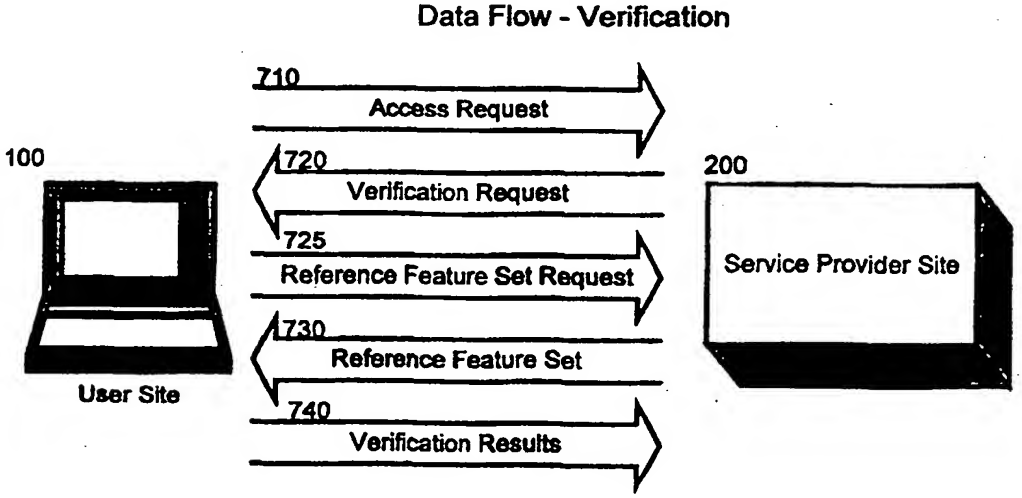
(71)(72) Applicants and Inventors: PHELPS, Barry, C. [US/US]; 10 Porchuck Road, Greenwich, CT 06831 (US). REDDI, Seenu, S. [US/US]; 15091 Clemons Circle, Irvine, CA 92604 (US).

(74) Agent: TALBOT, C., Scott; Morgan, Lewis & Bockius LLP, 1800 M Street, N.W., Washington, DC 20036 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: BIOMETRIC AUTHENTICATION SYSTEM AND METHOD



(57) Abstract

A method for biometric authentication of the identity of a user located at a user site (100) seeking access to services provided by a service provider (200) at a location different from the user site includes the steps of acquiring from the user a bid biometric feature set, transmitting to the user site a reference biometric feature set associated with the user and stored at a location remote from the user site, and comparing at the user site the bid feature set and the reference feature set.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

BIOMETRIC AUTHENTICATION SYSTEM AND METHOD

Background of the Invention

The invention relates to a method for authenticating the identity of users, and in particular to the authentication of users across networks, more particularly across the Internet.

In banking and other service industries, it is important to authenticate the identities of users of services. Authentication of identity historically involved comparison of a user's facial features to a reference photographic identification, such as a driver's license, by personnel of the service provider. With the advent of systems such as automated teller machines, remote door entry systems, and other access control devices unattended by personnel of the service provider, alternative methods were developed. These most commonly employ a physical access device, such as a security card or key, ATM card, etc. that incorporate machine readable identifying information. The authority of the bearer of the physical access device to use the device is verified by requiring entry of a code, such as a Personal Identification Number (PIN) that is presumed to be known only to the authorized bearer. The service provider grants access to a bearer of the access device who provides the code that correlates with the identifying information on the access device.

Such methods have the drawback that an unauthorized user may gain improper access to both the access device and the code. Systems were therefore developed to authenticate the identity of the user by means of uniquely-identifying biometric physical attributes of the user. These biometric attributes can include the user's voice, fingerprint, signature, iris, retina, and facial features. Biometric authentication involves two processes: an initial enrollment or registration process, and a verification process conducted each time the user seeks access to the service provider.

In the enrollment process, a reference biometric is acquired from the user, whose identity has been reliably established by other, conventional techniques

(such as personal comparison of facial features to photo identity cards by a service provider's personnel). The reference biometric is acquired by converting a biological feature or attribute (voice sample, finger print, signature, etc.) with an appropriate converter (microphone, scanner, etc.) into a set of numerical data, or biometric acquisition. Characteristic features are then extracted from the biometric acquisition to produce a feature set. In the context of, for example, voice print biometrics, a feature set is a parametric representation of the biometric voice sample, such as filter coefficients in a linear predictive coding approach. See, for example, Davis and Mermelstein, "Comparison of Parametric Representations for Monosyllabic Word Recognition in Continuously Spoken Sentences" (IEEE 1980), the disclosure of which is hereby incorporated by reference herein. Typically, multiple biometric acquisitions are taken and their feature sets combined into a composite, reference feature set. The reference feature set is then stored for future use.

To authenticate the user, another biometric is acquired from the user for extraction of a feature set for comparison to the reference feature set. The newly acquired biometric is referred to herein as a "bid" biometric. A bid feature set extracted from the bid biometric is then compared to the reference feature set, and a quality of comparison, or "score," indicative of the closeness of the match between the two feature sets is established. In the context of voice biometrics, the quality of comparison is a measure of the differences between the bid and reference feature sets, and therefore a low value for the quality of comparison is more indicative of close match than a high value. Therefore, a user's identification is authenticated (i.e. the user from whom the bid biometric was acquired is presumed to be the same user who provided the reference biometric, and is granted access to the service provider) when the quality of comparison has a value lower than a predetermined, threshold value. For other biometrics, such as fingerprints, higher values are more indicative of a match, and authentication would be based on the value of the quality of comparison exceeding a threshold value. For consistency and ease of reference in the present application, higher values of quality of comparison are considered to be

indicative of a better match, and authentication is based on the value of the quality of comparison exceeding a threshold value.

Known biometric authentication systems can be usefully classified and discussed according to the relative locations of the user, the service provider, the point of access to the service provider, the point at which the bid biometric is acquired, the point at which the bid feature set is extracted, the point at which the reference feature set is stored, the point at which the bid and reference feature sets are compared, and the point at which the verification is made (by evaluating the quality of comparison of the bid and reference feature sets). Unless the points of bid biometric acquisition, bid feature set extraction, reference feature set storage, and bid to reference feature set comparison are the same, there must be some transmission between points of one or more of the bid biometric, bid feature set, or reference feature set.

The assignee of the present application developed a secure door entry system with voice authentication. In this system, the point of access to the service provider is the doorway. The user is at the same location as the doorway when seeking admittance. Similarly, the service provider is at the same location (on the other side of the doorway). The reference feature set is stored at a location remote from the doorway, the biometric is acquired at the doorway (by a telephone handset), the bid feature set is extracted and compared to the reference feature set, at the remote site. The bid biometric acquisition is therefore transmitted (via a telephone line) in analog form from the doorway to the remote site.

U.S. Pat. Nos. 5,647,017 and 5,544,255 to Smithies disclose signature verification systems in which the bid biometric (signature) is acquired at a remote site (where the user is located) and transmitted to a host site (the point of access to the service provider) for verification. In these systems, the bid feature set is extracted at the user's site, and stored in a signature envelope along with the claimed identity of the user. The signature envelope is encrypted and sent to the host site (a second computer) for decryption and for subsequent comparison of the bid and reference feature sets. Thus, the bid feature set is transmitted from

the user site to the host site.

U.S. Pat. No. 5,280,527 to Gullman discloses a remote authorization system in which a security apparatus includes a biometric sensor for capturing biometrics such as voice print, fingerprint, or signature, PROM for storing a reference feature set generated from a biometric acquired in an enroll mode and a fixed code (e.g. PIN or account number). The security apparatus also includes a code generator that generates a time-varying code, a processor and a display. The security apparatus is disclosed as preferably being embodied in a self-contained, portable form, such as a smart card.

The system compares the bid biometric to the locally stored reference feature set, and generates a "correlation factor," or quality of comparison The correlation factor is compared to a threshold and if it exceeds the threshold, a security token is generated. The token combines the correlation factor, the fixed code, and the time varying code. The token is then displayed to the user, who can input it into an access device (e.g. ATM keypad). The access device transmits the security token to the host system, which decodes the token, determines from the fixed code whether the user is an authorized user, and whether the correlation factor exceeds the threshold. If so, access is granted. Thus, in Gullman's system the bid biometric is acquired, the bid feature set extracted, the reference feature set stored, the bid and reference feature sets compared, and the verification evaluation performed, at the same site as the user (in the smart card). The user is at the point of access (an ATM), while the service provider is remote.

U.S. Pat. Nos. 5,613,012 and 5,615,277 to Hoffman are directed to an authentication system in which a bid biometric (e.g. a fingerprint) is acquired, and the bid feature set extracted, at a biometric input device associated with a terminal at which the user is located. The terminal transmits the bid feature set to a remote data processing center (DPC), where it is compared to the reference feature set.

U.S. Pat. No. 5,706,427 to Tabuki discloses an authentication system for use in computer networks, in which the user (at a user host computer) seeks

services from a remote application server. The application server directs the user host to transmit a bid biometric (acquired at the host computer) to a verification server (at a third site different from that of the user or the application server), where the bid feature set is extracted and compared to the reference feature set and where the verification evaluation is performed.

It has become increasingly common for services to be accessed via computer networks, and with the explosive growth of the Internet has come a corresponding growth in the range of services that can be provided to users via the Internet. There is an attendant need for authentication by service providers of users who access their services via networks, particularly the Internet. Although some of the biometric authentication systems described above can be applied in the context of network, and Internet, service access, they suffer from shortcomings that can be particularly problematic in such contexts.

One of the well-recognized problems with the Internet is that data communication is often unreliable, in that data transmission speeds can vary widely, access by users to the Internet (via Internet Service Providers, or ISPs) can be difficult to establish and is often interrupted, requiring the user to reaccess the Internet. Similar problems can be encountered on other networks. This poses particular difficulties for biometric authentication systems. Biometric authentication is typically chosen because there is a high degree of concern with accurate identification of a user. Accordingly, in the operation of biometric systems a high degree of accuracy of identification verification is usually desired, necessitating that a bid feature set closely match the reference feature set. All biometrics suffer from a degree of variation between bid feature sets generated by a valid user. For example, voice biometrics vary for a given user by time of day, mood, state of health, etc. It is therefore not uncommon to produce false negatives, in which a valid user's bid feature set is rejected as being unacceptably different from the reference feature set. It is therefore common to allow a user to submit another bid biometric following a rejection. This can be repeated some predetermined number of times before the user is refused further bids and must resort to other avenues for access to the service provider. The

need to permit repeated bid biometric acquisition, bid feature set extraction, and feature set comparison operations in a single service provider access transaction makes network biometric authentication, especially on the Internet, unattractive because these operations are relatively likely to be interrupted. This would require the user to attempt (often unsuccessfully) to reestablish communication first with the Internet, then with the service provider's point of access and then to reinitiate the bid process.

In each of the references described above in which the reference feature set is stored at a site other than the user's site (i.e., all but Gullman), the bid biometric or bid feature set is transmitted to a site remote from the user for bid feature set extraction and/or bid-to-reference feature set comparison. If the verification evaluation produces a negative result, that information must be communicated back to the user's site so that another bid biometric can be acquired. Such systems are therefore susceptible to the interruption problem described above.

Gullman avoids the interruption problem by storing the reference feature set with the user (in the same smart card that contains the biometric sensor). However, Gullman's system suffers from two shortcomings. First, the user must have a physical token (the smart card). Second, the service provider does not have control over the reference feature set, since it is in the user's possession. Many, if not most, service providers would consider this to be unacceptable.

There is therefore a need for a biometric authentication system and process usable in the context of computer networks, particularly the Internet, that allows the service provider to maintain the reference feature set and that does not require transmission of the bid biometric or feature set to a site remote from the user for comparison to the reference feature set.

Summary of the Invention

The shortcomings of the prior art are overcome, and the need identified above is met, by the system and method of the invention. In the disclosed biometric authentication system and method, a user seeking access to a service

provider's service contacts an access point, such as a Internet site or page on the World Wide Web (WWW) and requests access. Identifying information (such as a name, account number, personal identification number (PIN), etc.) Is requested from the user. A reference biometric feature set maintained by the service provider (or a third party) remote from the user's site is transmitted (such as via the Internet) to the user's site. A bid biometric is acquired from the user and a bid feature set extracted from the bid biometric, at the user's site. The bid and reference feature sets are compared at the user's site, and a quality of comparison is determined and compared to a predetermined threshold value to determine, to a desired degree of certainty, whether the user's identity matches that of the user associated with the reference feature set. If the identities match, appropriate information indicative of the match is transmitted from the user site to the access point, which then grants the user access to the service provider. If the identities do not match, another bid feature set can be obtained from the user, compared to the reference feature set, and the resulting quality of comparison compared to the quality threshold. After a predetermined number of unsuccessfully attempted matches, the bid process can be terminated. This authentication process requires only a single transmission of a biometric feature set between the user site and access point. The bid feature set acquisition and comparison to the reference feature set, the quality of comparison calculation, and if necessary, subsequent bid feature set acquisition are all performed at the user's location. This renders the authentication process less vulnerable to interruption of communication between the user and the access point.

In the presently preferred embodiment, the biometric used for authentication is the user's voice. This permits the use of simple, inexpensive, and commonly and readily available biometric conversion hardware, such as a microphone.

Brief Description of the Drawings

Fig. 1 is a schematic illustration of a biometric authentication system.

Fig. 2 is a schematic illustration of a user site.

Fig. 3 is a schematic illustration of a service provider site.

Fig. 4 is a schematic illustration of the user and service provider sites.

Figs. 5A-C are flow diagrams of the service provider access procedure.

Figs. 6A-B are schematic illustrations of the flow and contents of data exchanged by the user and service provider sites during the enrollment process.

Figs. 7A-B are schematic illustrations of the flow and contents of data exchanged by the user and service provider sites during the verification process.

Detailed Description of Presently Preferred Embodiments

A biometric authentication system embodying the principles of the invention is illustrated in schematic form in Fig. 1. The system includes a user site 100, which can communicate via a network, for example the Internet 10, with a service provider site 200. Service provider site 200 conceptually includes a service provider access site 210, a service provider service site 220, and a verification / storage site 230. In broad terms, the user seeks access to services available from service site 220 by contacting access site 210, which initiates communication between user site 100 and verification / storage site 230, either directly or via access site 210.

User site 100 generally consists of a personal computer equipped with appropriate hardware and software to enable acquisition and manipulation of biometrics, communication with access site 210, and execution of biometric verification processes through interaction with access site 210 and/or verification site 230. As shown in Fig. 2, user site 100 can include user input device(s) 110, biometric sensor or converter 120 for acquiring biometrics from the user, output device(s) 130, processor (with RAM) 180, communications device 150, software and data storage 145, all of which can communicate with each other via, for example, communication bus 170.

User input device(s) 110 can include a keyboard and a pointing device (mouse, joystick, track pad, etc.). Biometric converter 120 can include any suitable device for acquiring a selected biometric. In the illustrated embodiment,

the selected biometric is a voice print, and biometric converter 120 is therefore a microphone. Any suitable apparatus and process can be used for acquiring voice prints, extracting reference and bid feature sets, comparing feature sets, evaluating the quality of the comparison, setting threshold values, and comparing quality of comparison to thresholds. Such suitable apparatuses are available for selection by the artisan, and neither their selection nor the details of their operation form a part of the invention. Other devices can be used for other biometrics, such as a digitizing pad or scanner to acquire signatures, a camera to acquire facial features, a scanner to acquire fingerprints, etc.

Output device(s) 130 can include a visual display, auditory output device such as a speaker, and physical output device such as a printer. Communications device 150 can include any suitable device for communication with the network on which the service provider access site is resident, such as a modem for communication via analog data lines with an ISP, a network interface to the network containing the access site or a local area network having capabilities for communication with the Internet. Storage 145 can include any suitable mass storage device, such as magnetic or optical disk drive, etc., on which can be stored software and data associated with the biometric authentication process and from which the software and data can be retrieved and loaded into RAM or other location suitable for execution and processing by processor 180.

As illustrated in Fig. 3, service provider site 200 can include communications device 240, processor 250, services 280, reference feature sets storage 260 and software for downloading storage 270. The communications device 240 provides the ability to communicate with the network, preferably the Internet 10, communicating requests for access to the services 280 as well as downloading software and reference feature sets. The processor 250 processes requests for access, requests for software to be downloaded and requests for reference feature sets for be downloaded. Services 280 can consist of any services the service provider is offering to the user, such as banking services, once access to the service provider has been authenticated.

Fig. 4 illustrates schematically user site 100 and service provider site 200. In the illustrated embodiment, each user site has a computer including CPU 185, user interface 190, primary memory (RAM) 140, user communications interface 151 for communication with the service provider 200 via the communication network 10, and additional memory 160 for loading software for execution by CPU 180. The software components include software that is already resident at user site 100 before accessing the service provider site 200, such as an operating system 162, and network navigation / interface software, such as WWW browser program 164.

In the illustrated embodiment, service provider site 200 has a computer including CPU 290, primary memory (RAM) 292, communications interface 294 for communicating with the user sites 100 via the communications network 10, and additional memory 295 for loading software for execution by CPU 290. The software components include server interface software and/or data 296, such as hypertext documents encoded in Hypertext Markup Language (HTML), which present the Web page to the user. Thus, user site 100 and service provider site 200 communicate via interaction between browser program 164 and the server interface 296, i.e. by the browser program reading the HTML encoded Web page. The authentication process is implemented in software which has components at both the service provider site 200 and the user site 100, which components operate as a layer or interface between the browser and the HTML.

The user site software component 165 is downloaded from the service provider site 200 during the enrollment process, as described below. In the illustrated embodiment, the downloaded software includes native code 168, which contains the functions Verify() and Enroll(), 168a and 168b, respectively, and browser interface 166. Browser interface 166 provides an interface between the native code and the browser. The service provider site software component 298 is an applet that can be invoked through the Web page via the browser. This applet in turn communicates with the browser interface software to initiate execution of the native code. In one embodiment, browser interface 166 is implemented as a Netscape plug-in and the service provider site software

component 298 is correspondingly implemented as an applet coded in the Java programming language. In a second, presently preferred embodiment, browser interface 166 is implemented as a Microsoft ActiveX program (OCX), and the service provider site software component 298 is correspondingly implemented as ActiveX control.

The operation of the disclosed authentication system will now be described. The service provider access procedure 500 of the illustrated embodiment is illustrated in Fig. 5A. The process begins when the user initiates access to the service provider's access site on the WWW at step 502. The service provider determines at step 504 if the user is a new user to the service. If the user is new, then the enrollment process is initiated at step 508 with a New User Request to the service provider 200. The service provider 200 assigns a User ID for this user at step 509, then transmits a New User Download at step 510, which provides the user site software component 165. The service provider then generates a request for enrollment at step 580. The user in turn initiates the enrollment procedure at step 590.

Enrollment procedure 590 is shown in more detail in Fig. 5B. Enrollment process 590 begins with initiation of the Enroll() function 168a at step 592. The Enroll() function acquires from the user at step 594 several biometric samples, from each of which is extracted a feature set. The feature sets are combined to generate a composite, reference feature set at step 596. The reference feature set is then uploaded at step 598 to the service provider for storage in the reference feature set repository. Upon successful completion of the enrollment process, control of the process is returned to the access procedure at step 599.

The flow and content of data exchanged by user site 100 and service provider site 200 relating to the enrollment process 590 is illustrated schematically in Figs. 6A and 6B. When a user new to the service provider requests access, the user is prompted to issue a New User Request 650. As shown in Fig. 6B, New User Request 650 includes a block of identifying information 652 about the user (such as the user's name, address, account number with the service provider, etc.). The service provider assigns a User ID

664 for the user, and then downloads to the user a New User Download 660. Download 660 includes User ID 664, the user site software component 165, and information relating to the verification process, such as a default maximum number of verification attempts allowed 662, and default quality of comparison threshold 663. After the downloaded software is installed and executed, the reference feature set 672 is generated, and an enrollment upload 670 is sent to the service provider. Enrollment upload 670 includes User ID 664 and reference feature set 672. The service provider then stores reference feature set 672.

After enrolling, the user can access the service provider's service site, subject to the verification process. As shown in Fig. 5A, after determining that the user is not a new user at step 504, the verification process is initiated at step 530 with an Access Request transmitted from user site 100 to service provider 200. In response, the service provider requests verification at step 540 by transmitting Verification Request 720. This in turn initiates the verification process at step 550.

Verification procedure 550 is shown in more detail in Fig. 5C. Verification procedure 550 begins with initiation of the Verify() function 168b at step 551. The Verify() function generates a request to the service provider for this User ID's reference feature set. The reference feature set is downloaded to the user site in step 552. The Verify() function then acquires from the user a bid biometric sample in step 553, from which a bid feature set is extracted. The bid feature set is compared to the reference feature set at step 554, and a quality of comparison, or score, is calculated at step 555. The quality of comparison represents a goodness of fit, or match, between the bid and reference features sets, and correlates with the likelihood that the user is the person from whom the reference feature set was generated.

The quality of comparison is then compared at step 556 to a threshold value to determine if the user should be authenticated. The threshold is set at a predetermined value, which value is selected to strike the balance preferred by the service provider between having a high degree of confidence that the user is authentic and having authentic users incorrectly rejected. If the quality of

comparison exceeds the threshold, the verification process returns that the user should be authenticated at step 557. If the quality of comparison does not exceed the threshold, then the Verify() function checks to see how many times the user has thus far attempted verification at step 558. If the number of bids does not exceed the maximum number of allowed attempts, the user can generate a new bid by acquiring and extracting a new bid biometric, as shown by loop 501 in Fig. 5C. If the quality of comparison of the bid biometrics never exceeds the threshold and the user exceeds the maximum allowed attempts, then "user not authenticated" is returned at step 559, and the user is not allowed access to service provider site 200.

The flow and content of data exchanged by user site 100 and service provider site 200 relating to the verification process 550 is illustrated in Figs. 7A and 7B. When a user known to the service provider requests access, the user site 100 sends an Access Request 710 to service provider site 200. As shown in Fig. 7B, Access Request 710 includes User ID 664. Service provider site 200 then transmits a Verification Request 720 to user site 100. Verification Request 720 can include a call to Verify() 722, the maximum allowable number of bids for this access attempt 724, and the minimum quality of comparison threshold required for this access attempt 726. Maximum allowable number of bids 724 and minimum quality of comparison threshold 726 are optional data, to be used if the service provider wishes to override the default maximum allowable number of bids 662 and default minimum quality of comparison threshold 663 downloaded in the New User Download 660. Request 725 for the bid user's reference feature set is then transmitted to service provider site 200, and reference feature set 730 is downloaded. Once verification process 550 is complete at user site 100, verification result 740 (User Authenticated 742 or User Not Authenticated 743) is returned to service provider 200, and the user is granted or denied access accordingly.

The disclosed, presently preferred embodiment is merely illustrative of the principles of the present invention, and many variations on the disclosed features and processes are contemplated and will be apparent to the artisan. For

example, although the use of voice biometrics is disclosed, any other biometric can be used. All of the functional elements of the service provider's site (access site, service site, storage site, verification site) can be located at the same physical location or network site, or can be dispersed across a network (including a LAN, WAN, or the Internet). Although it is assumed that the service site is under the direct control of the service provider, the other elements or functions (access, storage, verification) can be under control of third parties or the service provider. Although it is preferred to store, and transmit to the user site, a reference feature set, it is contemplated that reference biometrics could be stored and transmitted instead.

It is also preferred to conduct at the user site the steps of comparing the bid and reference feature sets, determining whether the quality of comparison exceeds the desired threshold, and acquiring additional bid biometrics, extracting additional bid feature sets, and conducting additional comparisons, so that the only transmissions required between the user and service provider sites is that of the reference feature set to the user site and that of the authentication determination to the service provider site. However, it is also contemplated that some of these steps could be performed at the service provider site, albeit at the cost of additional transmissions and attendant risk of interruption. For example, the quality of comparison could be transmitted to the service provider site, where it could be compared to the threshold, and if the threshold is not met, an instruction transmitted back to the user site to acquire another bid biometric, extract another bid feature set, perform another comparison, and transmit to the service provider site another quality of comparison.

What Is Claimed Is:

1. A method for biometric authentication of the identity of a user located at a user site seeking access to services provided by a service provider at a location different from the user site, the user having associated therewith a reference biometric feature set stored at a location remote from the user site, comprising the steps of:

acquiring from the user a bid feature set;

transmitting the reference feature set to the user site; and

comparing at the user site the bid feature set and the reference feature set.

2. The method of claim 1, further comprising the steps of:

determining a quality of comparison of the bid and reference feature sets;

comparing the quality of comparison to a predetermined threshold; and

granting the user access to the service provider's services if the quality of comparison exceeds the threshold.

3. The method of claim 2 wherein said steps of determining a quality of comparison and comparing the quality of comparison to the threshold are conducted at the user site.

4. The method of claim 1 further comprising the steps of:

transmitting from the user site to a point of access to the service provider a request for access to the service provider; and

transmitting to the user a request to supply the bid feature set.

5. The method of claim 4 wherein said point of access and said user site are sites on a computer network and said step of transmitting said request for access includes transmitting said request via said network.

6. The method of claim 1 wherein said reference feature set is transmitted to the user site via a network.

7. The method of claim 5 wherein said network is the Internet.

8. The method of claim 6 wherein said network is the Internet.

9. A method for biometric authentication of the identity of a user purporting to be an authorized user of the services of a service provider, the service provider having a point of access located at an access site, the user being located at a user site remote from the access site, the authorized user having associated therewith a reference feature set stored at a location remote from the user site, comprising the steps of:

transmitting from the access site to the user site a request to acquire from the user a bid feature set;

transmitting from the access site to the user site the reference feature set;

accepting from the user site a value indicative of the quality of a comparison of the reference feature set to the requested bid feature set; and

granting access to the user if said value exceeds a predetermined threshold.

10. The method of claim 9 wherein the access site and the user site are sites on a computer network and said reference feature set is transmitted via the network.

11. The method of claim 10 wherein the network is the Internet.

12. A method for biometric authentication of the identity of a user located at a user site and seeking access to the services of a service provider, the service provider having a point of access located at an access site remote from the user site, the user having associated therewith a reference feature set stored at a

location remote from the user site, comprising the steps of:

transmitting from the user site to the access site a request for access to the service provider;

receiving at the user site from the access site a request to acquire from the user a bid feature set;

acquiring from the user a bid feature set;

receiving at the user site from the access site the reference feature set;

comparing the bid feature set to the reference feature set and determining a quality of comparison; and

transmitting from the user site to the access site an indication of the quality of the comparison.

13. The method of claim 12 further comprising the steps of:

comparing the quality of comparison to a predetermined threshold, and, if the quality of comparison does not exceed the threshold,

acquiring from the user a second bid feature set.

14. The method of claim 12 wherein the access site and the user site are sites on a computer network and said reference feature set is transmitted via the network.

15. The method of claim 14 wherein the network is the Internet.

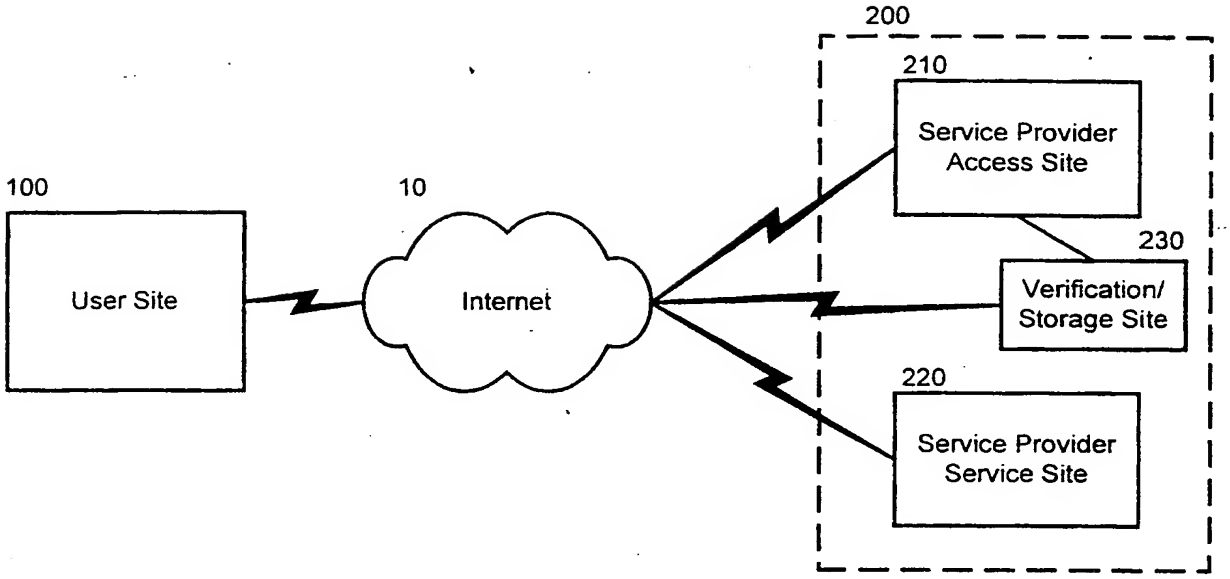


Fig. 1

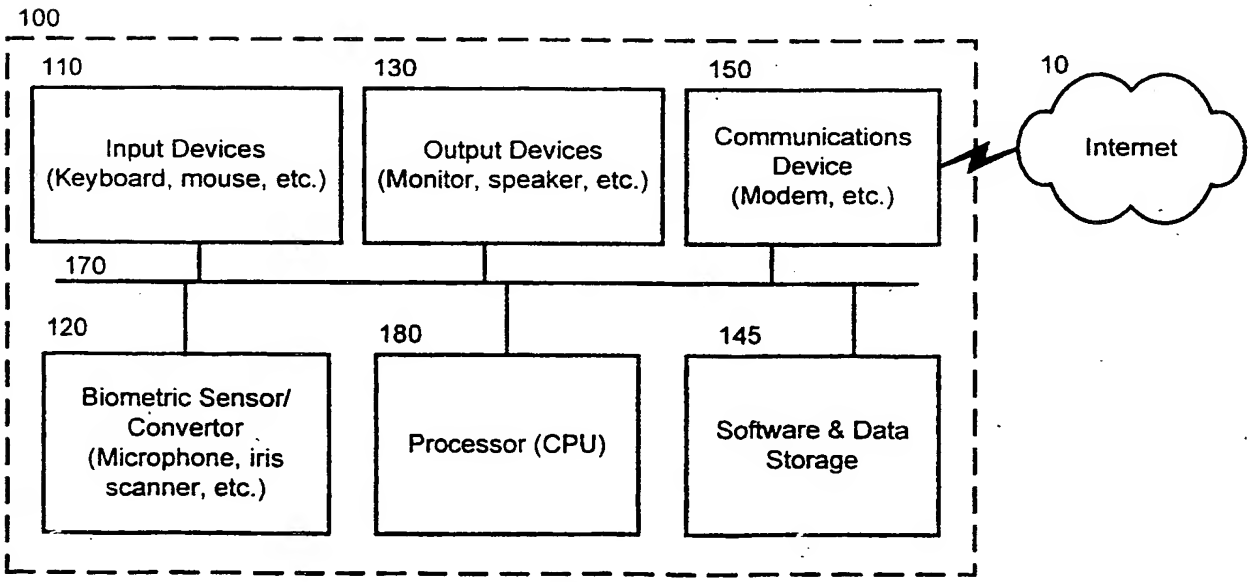


Fig. 2

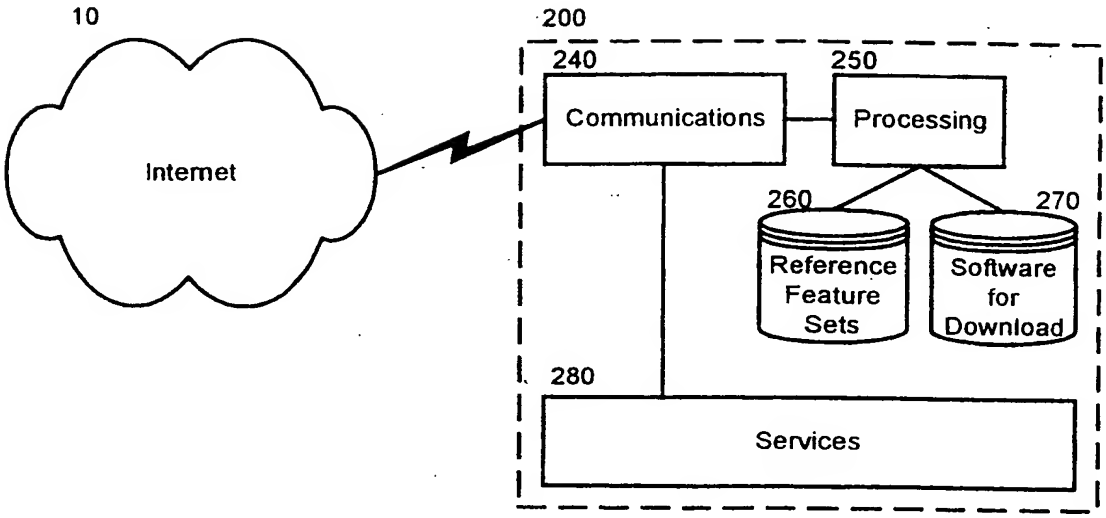


Fig. 3

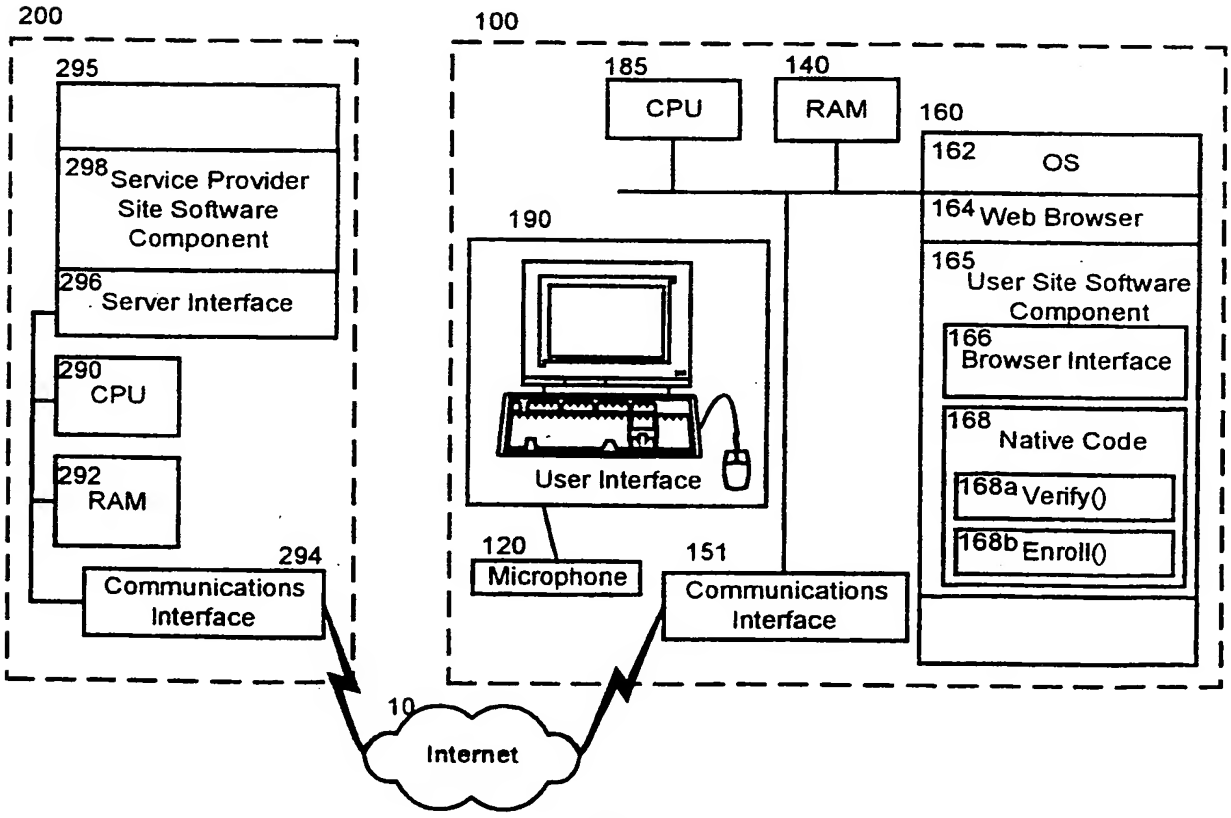


Fig. 4

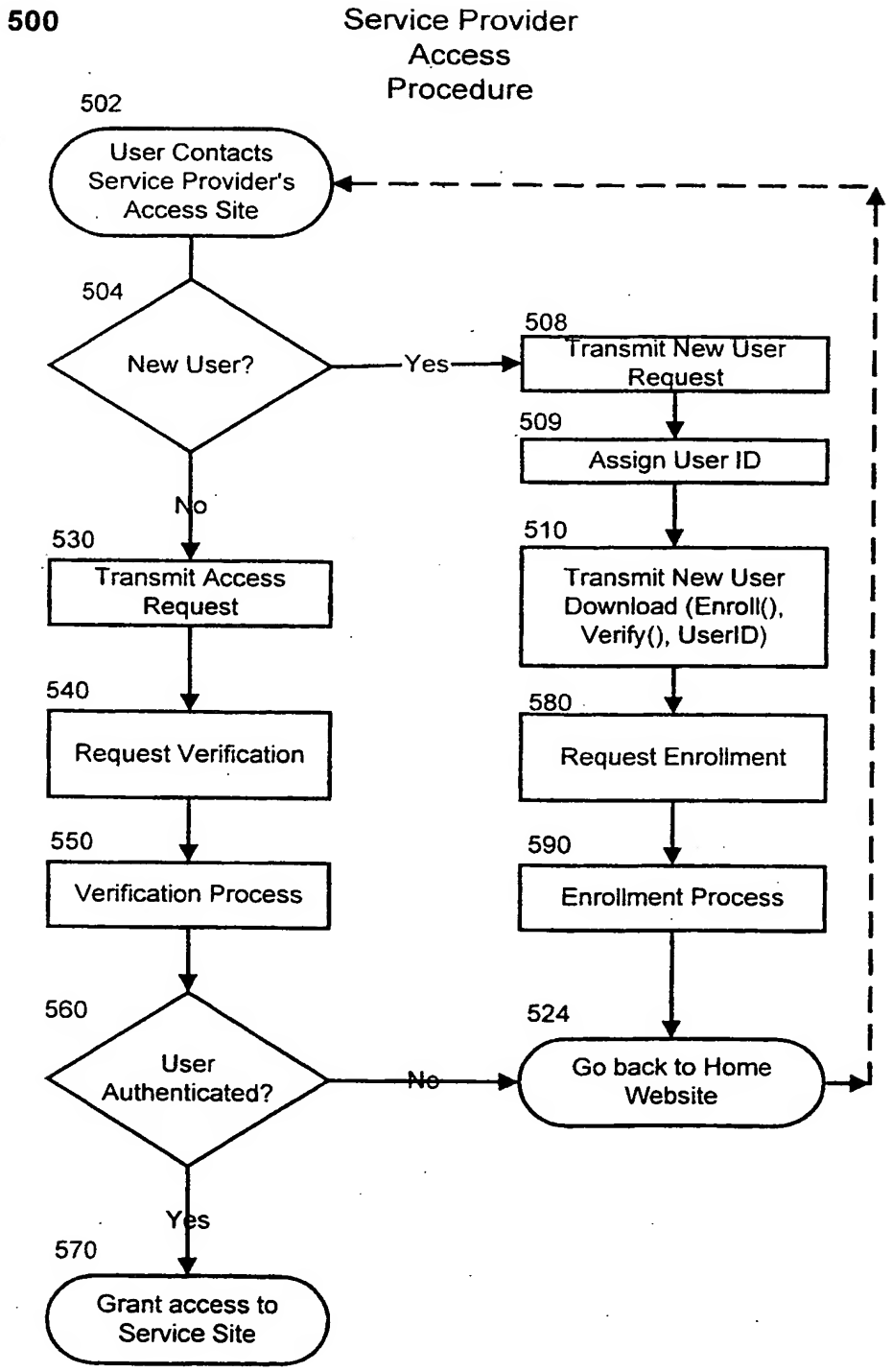


Fig. 5A

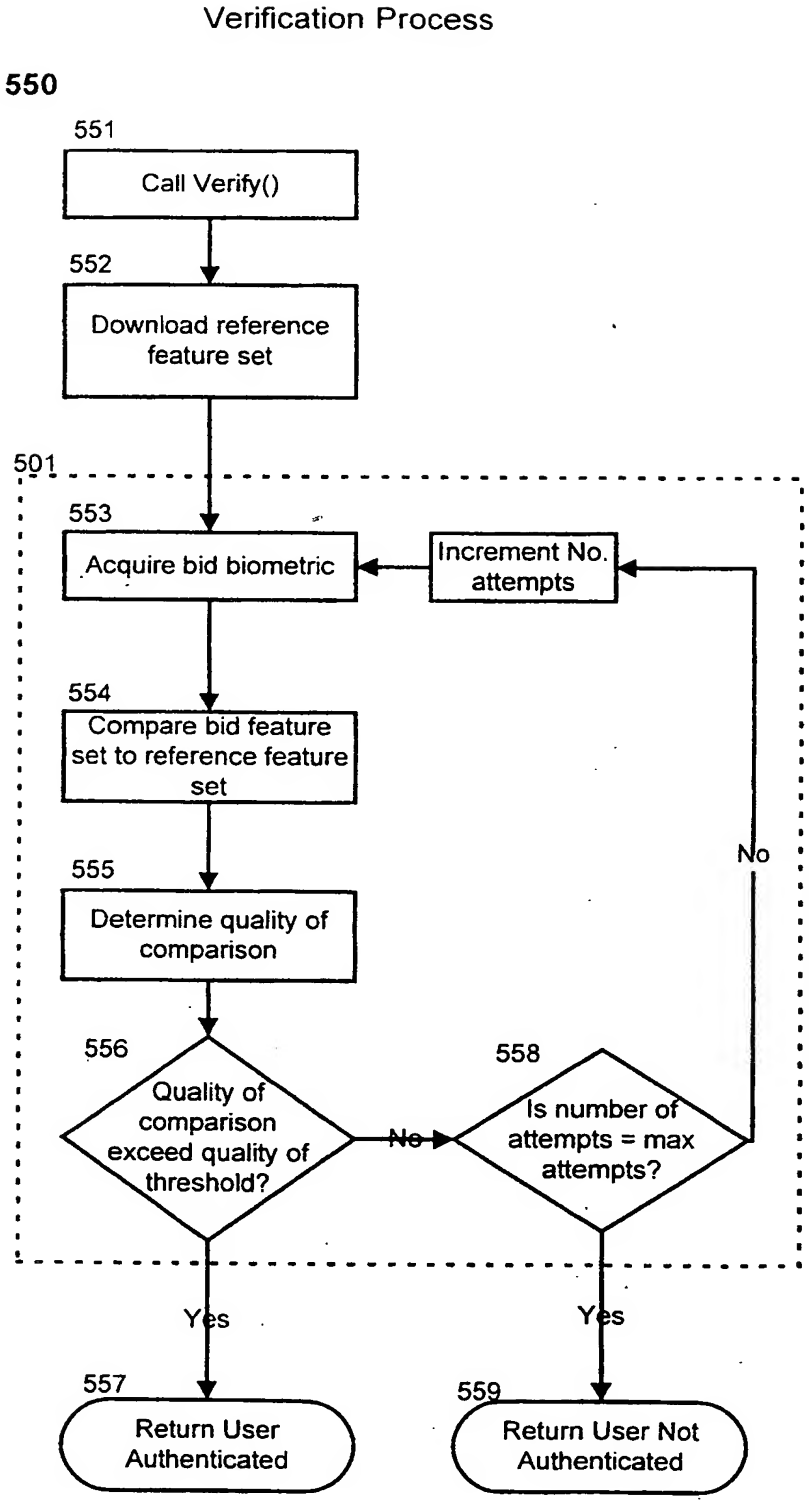


Fig. 5C

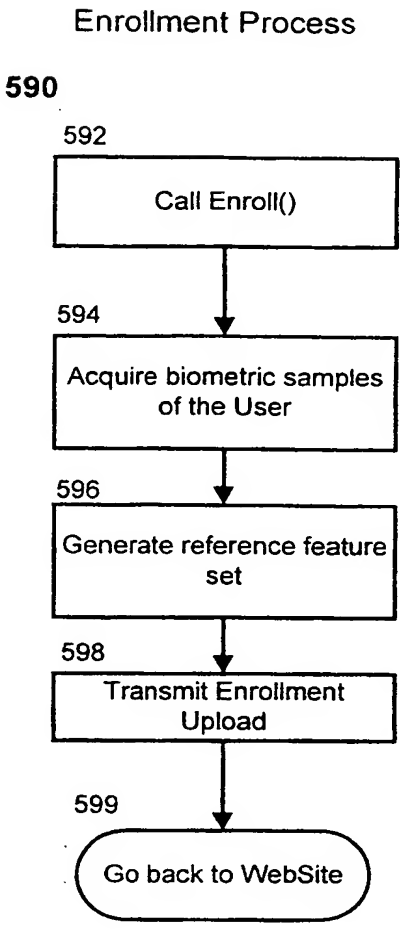


Fig. 5B

Data Flow - Enrollment

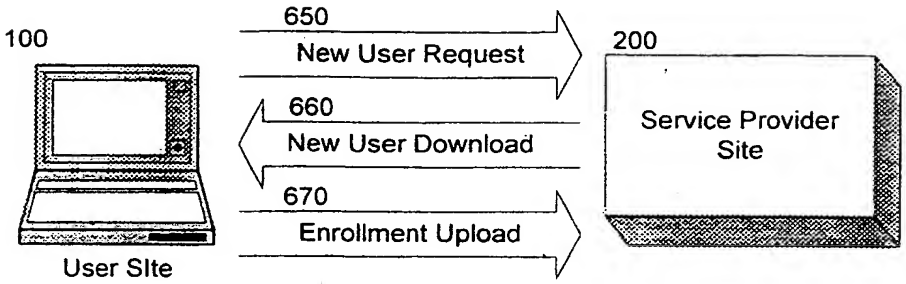


Fig. 6A

650 New User Request

652 Identifying Information

660 New User Download

664 User ID	165 User Site Software Component	662 Maximum allowed verification attempts	663 Quality of Comparison Threshhold

670 Enrollment Upload

664 User ID	672 Reference Feature Set

Fig. 6B

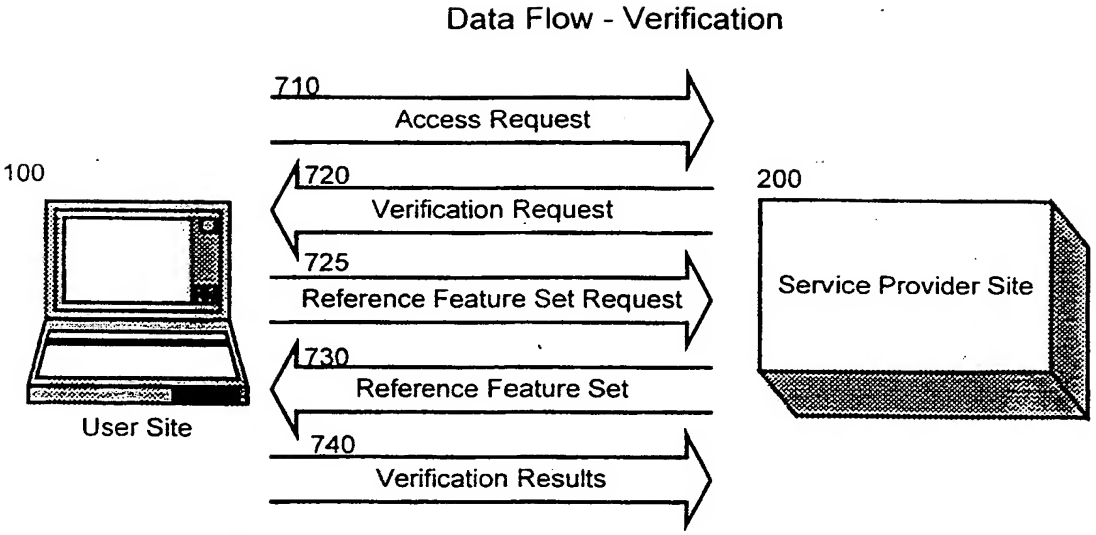


Fig. 7A

710 Access Request

664 User ID

720 Verification Request

722 Call to Verify()	724 Maximum allowable attempts	726 Quality of Comparison Threshhold

725 Reference Feature Set Request

664 User ID

730 Reference Feature Set

Reference Feature Set

740 Verification Results

742 User Authenticated or 743 User Not Authenticated

Fig. 7B

INTERNATIONAL SEARCH REPORT

Inte. .tional Application No
PCT/US 99/01727

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	STOCKEL A: "SECURING DATA AND FINANCIAL TRANSACTIONS" 18 October 1995 , PROCEEDINGS OF THE 29TH. ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, SANDERSTEAD, GB, OCT. 18 - 20, 1995, NR. CONF. 29, PAGE(S) 397 - 401 , SANSON L D (ED) XP000575565 see abstract; figure 1 see column 2, line 10 - column 3, line 8 see column 5, line 33 - line 46 see column 7, line 1 - column 9, line 16	1,6,8
Y		2-5,7, 9-12,14, 15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 May 1999	26/05/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte .ational Application No
PCT/US 99/01727

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 86 06527 A (QUANTUM FUND LTD) 6 November 1995 see abstract; figure 7 see page 2, line 7 - line 24 see page 4, paragraph 4 - paragraph 5 see page 13, line 4 - page 14, column 20	1-3
A		4,9,12

X	WO 96 18169 A (KRETZSCHMAR LOREN ;DAVIS VICTORIA (US)) 13 June 1996 see abstract; claims 1,3,4; figure 1 see page 3, line 8 - page 4, line 23 see page 5, line 9 - page 6, line 33 see page 10, line 16 - page 11, line 18	1,6
A		4,5, 7-12,14, 15

Y	US 5 386 104 A (SIME IAIN R F) 31 January 1995 see abstract; figures see column 1, line 55 - column 2, line 42 see column 3, line 12 - column 5, line 65	2-5,7, 12,14,15
A		13

Y	US 5 229 764 A (MATCHETT NOEL D ET AL) 20 July 1993 see abstract; figures see column 3, line 10 - line 52 see column 4, line 55 - column 7, line 5 see column 8, line 12 - column 9, line 9 see column 10, line 10 - column 11, line 15	9-11
A		1,12,13

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ational Application No
PCT/US 99/01727

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 8606527 A	06-11-1986	EP 0218668 A	22-04-1987
		GB 2174831 A,B	12-11-1986
		JP 62502575 T	01-10-1987
		US 4805223 A	14-02-1989
WO 9618169 A	13-06-1996	AU 4894796 A	26-06-1996
US 5386104 A	31-01-1995	EP 0652540 A	10-05-1995
		JP 7192164 A	28-07-1995
US 5229764 A	20-07-1993	NONE	

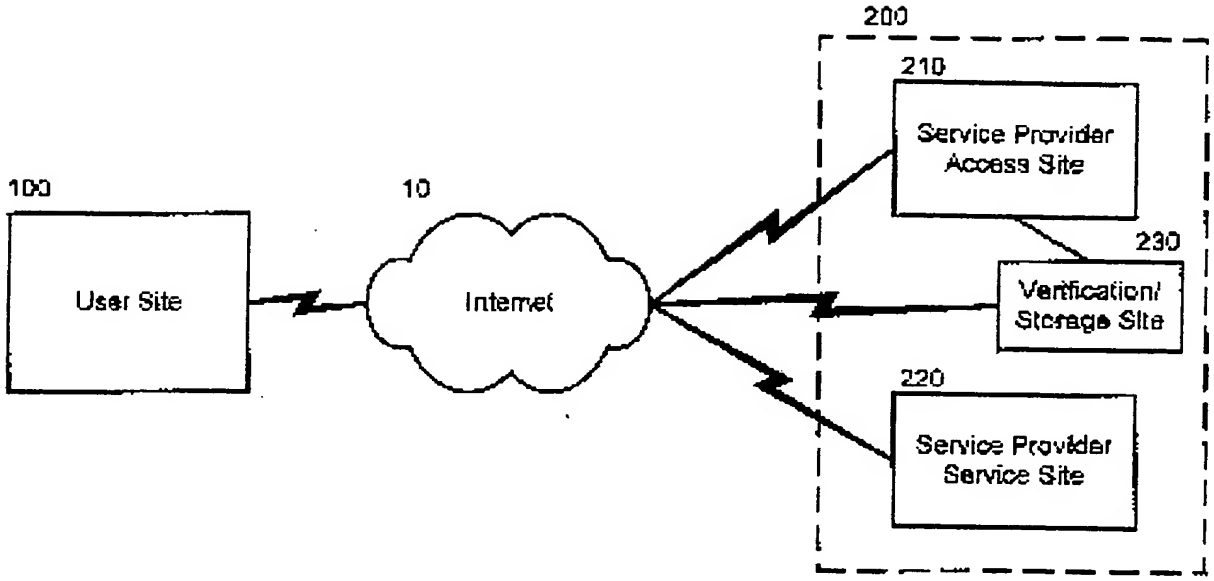


Fig. 1

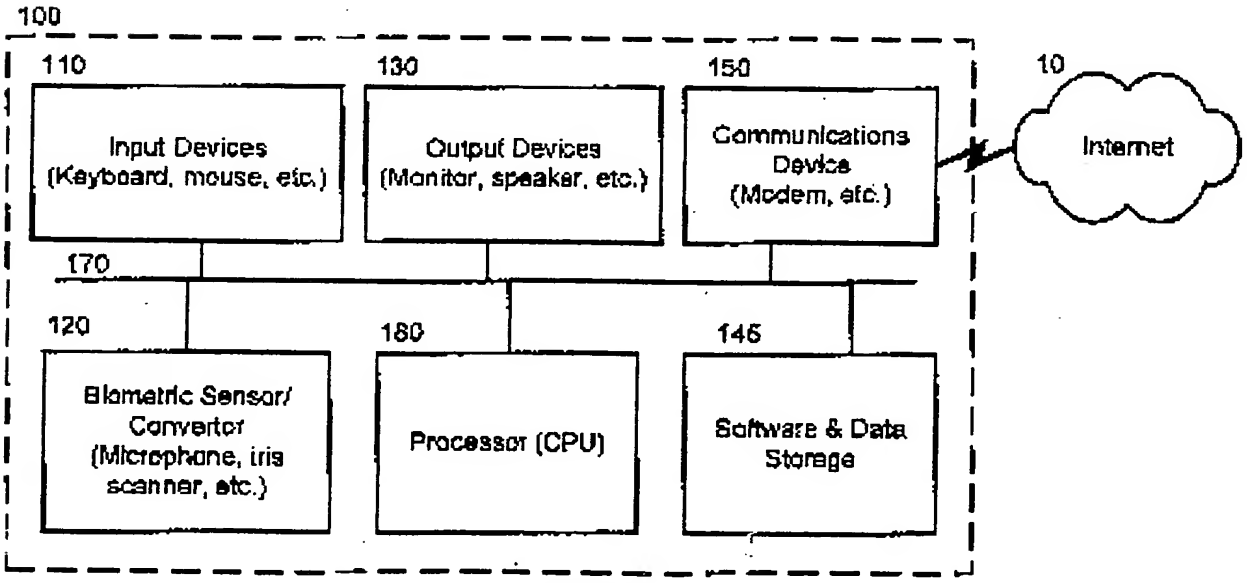


Fig. 2

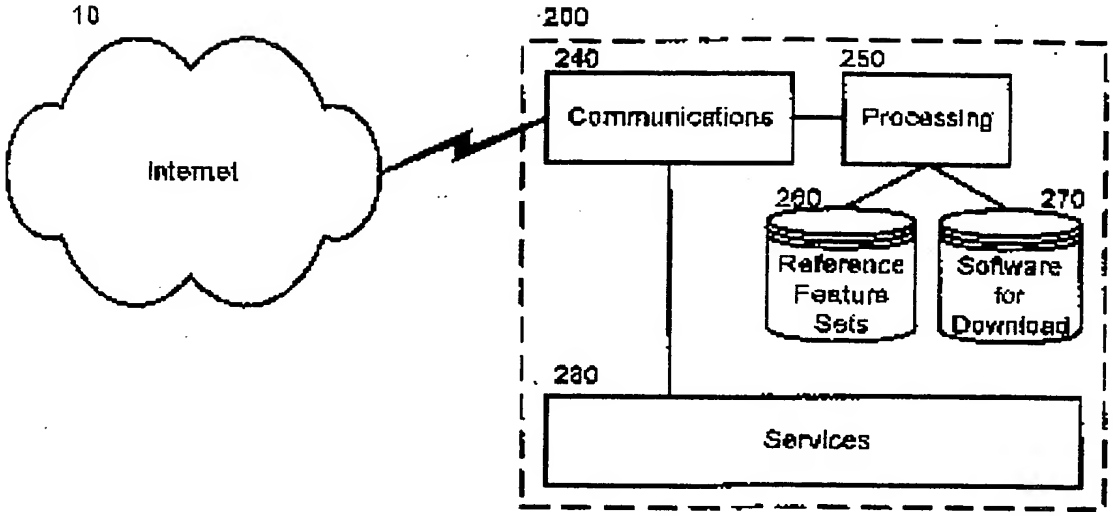


Fig. 3

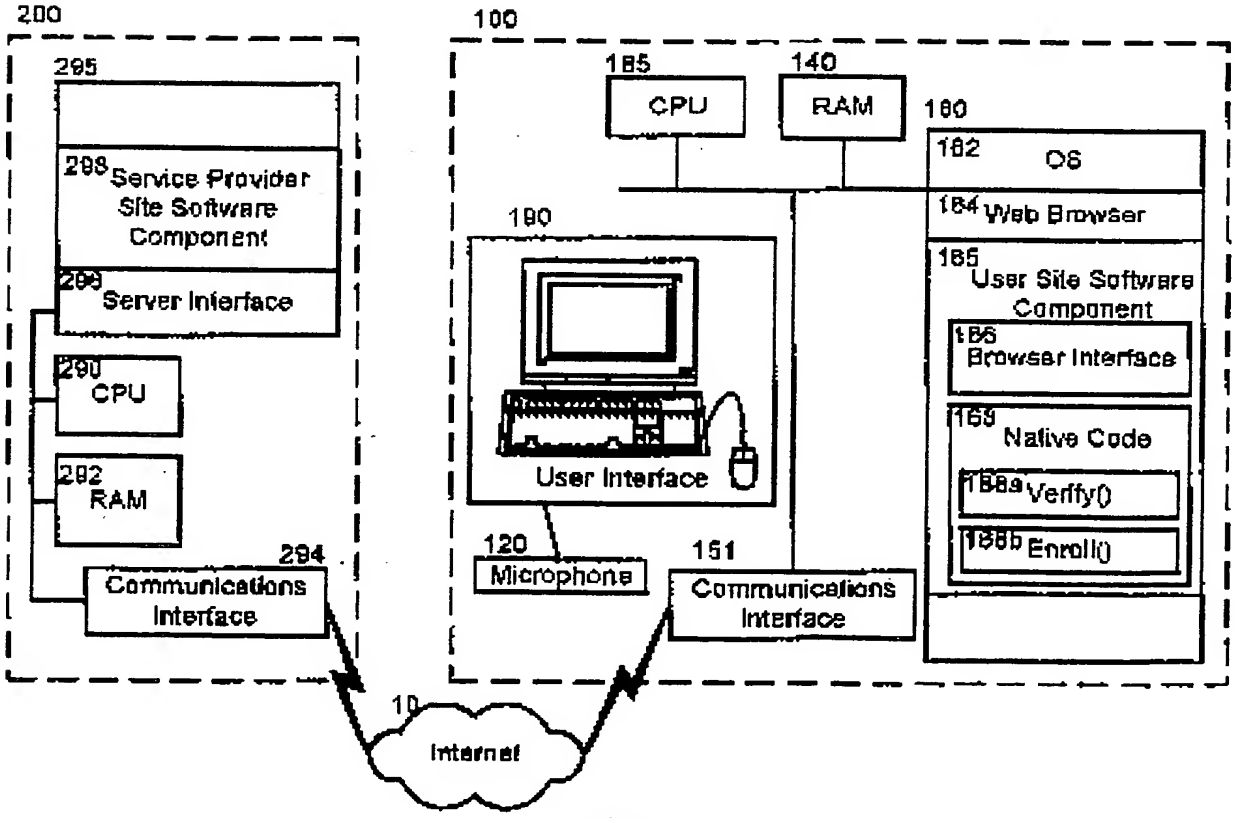


Fig. 4

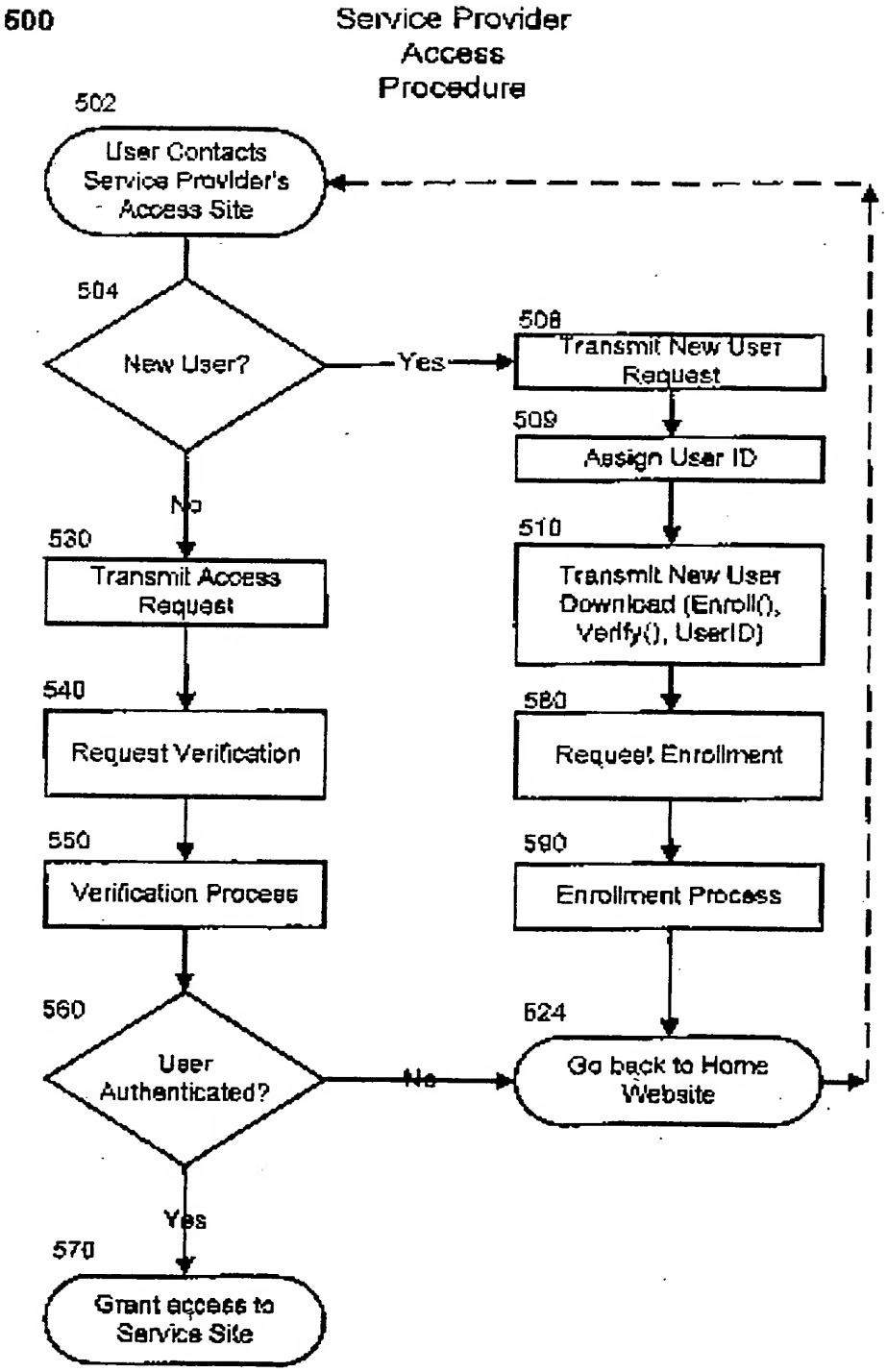
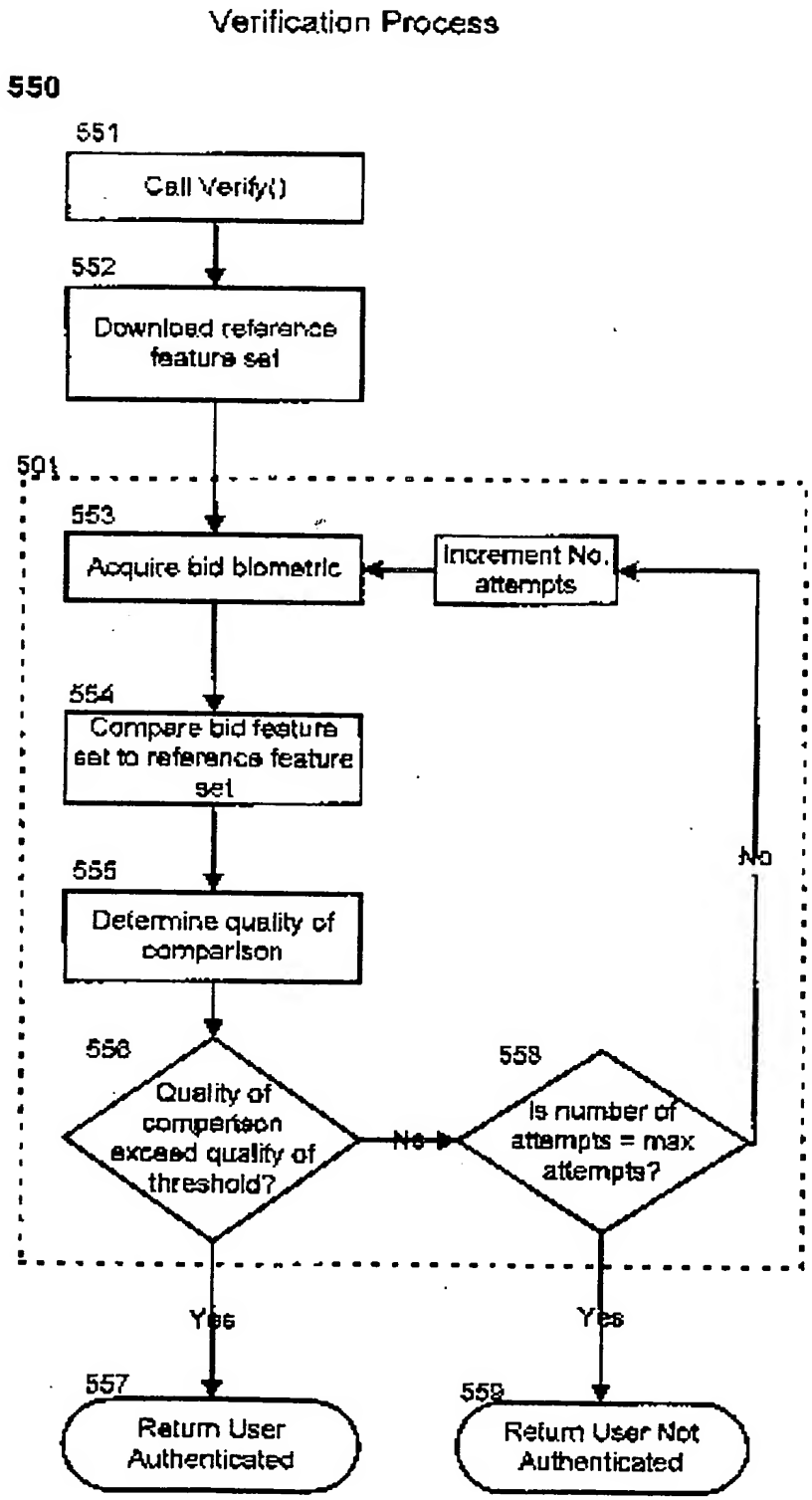


Fig. 5A



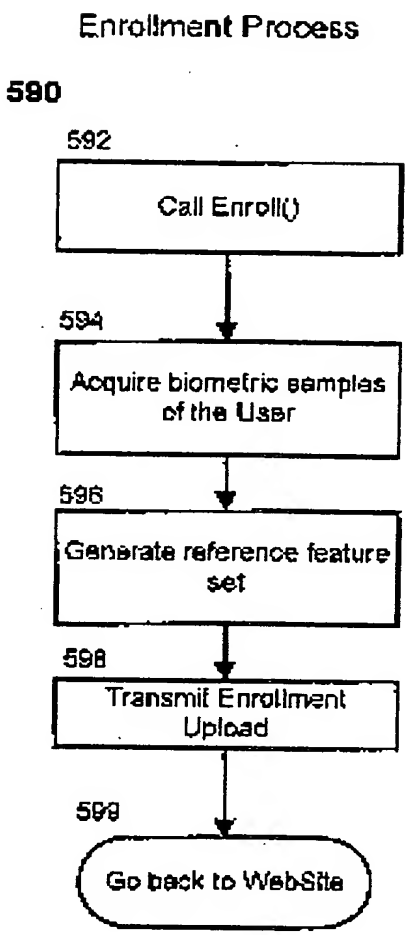


Fig. 5B

Fig. 5C

Data Flow - Enrollment

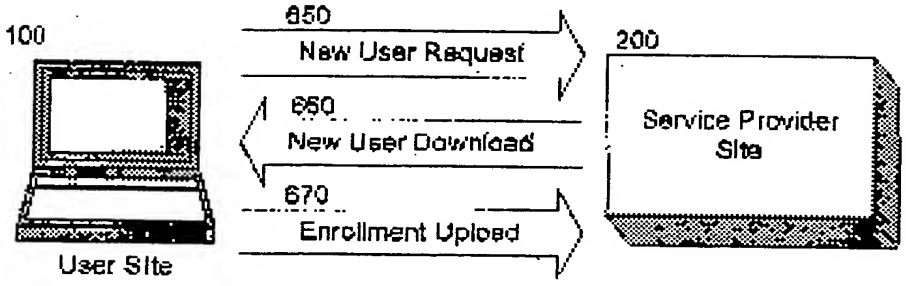


Fig. 6A

650 New User Request

652 Identifying Information

660 New User Download

664 User ID	165 User Site Software Component	662 Maximum allowed verification attempts	663 Quality of Comparison Threshhold

670 Enrollment Upload

664 User ID	672 Reference Feature Set

Fig. 6B

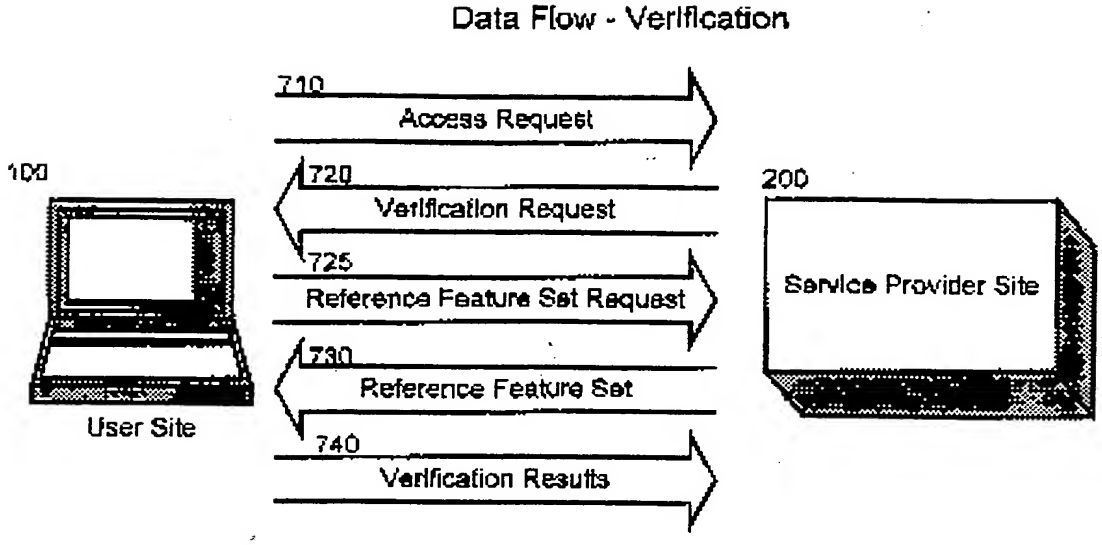


Fig. 7A

710 Access Request

664 User ID

720 Verification Request

722 Call to Verify()	724 Maximum allowable attempts	726 Quality of Comparison Threshhold

725 Reference Feature Set Request

664 User ID

730 Reference Feature Set

Reference Feature Set

740 Verification Results

742 User Authenticated or	743 User Not Authentfcated

Fig. 7B